

UNITED STATES PATENT APPLICATION

OF

Vyacheslav S. Belenko and Vsevolod M. Kuzmich

For

COPY PROTECTION METHOD

FOR DIGITAL MEDIA

OIPE JC87
APR 24 2002
PATENT & TRADEMARK OFFICE

CROSS-REFERECNE TO RELATED APPLICATIONS

[0001] This application claims the benefit of U.S. Provisional Application No. 60/265,884, filed on February 5, 2001, in the name of inventors Vyacheslav S. Beleko and Vsebolod M. Kumich, titled "Copy Protection Architecture for Digital Media", which is hereby incorporated by reference as if fully set forth herein.

BACKGROUND OF THE INVENTION

Field of the Invention

[0002] The present invention relates to media copy protection, and more particularly, to a digital media copy protection method that provides a secure copy control of the digital media using hybrid cryptographic and watermarking techniques and an authenticated handshake protocol.

Discussion of the Related Art

[0003] Communication systems such as computer networks, telecommunication systems, and other systems are increasingly using cryptography for the security of information. There are two main classes of cryptographic systems: symmetric key and public

key cryptographic systems. In a symmetric key cryptographic system, a symmetric (secrete) key is used for both of data encryption and decryption processes. There are several efficient implementations of the symmetric key cryptographic system, but the actual key managements of such implementations are often troublesome.

[0004] On the other hand, in a public key cryptographic system, the data encryption and decryption processes are independent from each other. That is, the data encryption process requires a public key, often designated as e, while the data decryption process requires a different (but mathematically related) private key d. Therefore, an entity being possessed of the public key may encrypt a plaintext, which is the original form of a message, but the entity may not be able decrypt a ciphertext, which is the encrypted form of the message.

[0005] If an entity selects a public key and publishes the public key, anyone is able to use the key to encrypt one or more messages for the entity. Then the entity keeps his private key secret so that he or she is the only one who can decrypt the ciphertexts of the messages. The implementations of the public key cryptographic system are currently less efficient than those of the symmetric key cryptographic systems, but they are much safer.

[0006] In a hybrid cryptographic system, a plaintext is encrypted with a symmetric key corresponding to a symmetric algorithm. The symmetric key is then encrypted with a public key corresponding to a public algorithm. When a receiver receives the public key-encrypted symmetric key and the symmetric key-encrypted data, the receiver initially decrypts the symmetric key by using his own private key. Subsequently, the receiver decrypts the encrypted data by using the decrypted symmetric key. The processes of obtaining the original data in a hybrid cryptographic system are usually faster than those of the public key cryptographic system. In addition, a hybrid cryptographic system may allow using a different symmetric key each time, considerably enhancing the security of the symmetric algorithm. For that reason, the hybrid cryptographic systems are ideal for transferring the protected media data safely to a receiver.

[0007] Watermarking is a technology, in which copyright information (information indicating a copy guard) is expressed by a watermark superposed in media data. Such information is embedded into various media data including image data and sound data, and it should be invisible and inaudible to a human observer. The purpose of superposing a watermark in the media data is to provide a proof of a copyright so that an illegal use and copy of the media data can be prevented. Therefore, the

copyright information should stay stable in a host signal even when the host signal is subjected to any data process.

[0008] The technique for superposing a watermark in the media data depends on the size of the watermark data and the invariance of the watermark data to any data process of a host signal. There is a watermark inherent trade-off between the human perceptibility, bandwidth, and robustness (i.e., the degree to which the data are immune to be attacked or transformations that occur to the host signal through a normal usage). The more data to be superposed, the less secure the encoding process is. The less data to be superposed, the more secure the encoding process is.

[0009] In a cryptographic system, an entity ensures whether other entities are approved through an authentication process. The authentication process is usually implemented in the form of a handshake protocol. During a handshake process, authenticating entities exchange the randomly generated data together with their identity identifications. After the result of the handshake process is analyzed, the decision of authenticating of a counterpart entity is made. In order to make the handshake process more secure and resistant to any man-in-the-middle attacks, a public key cryptographic system is often used.

SUMMARY OF THE INVENTION

[0010] Accordingly, the present invention is directed to a copy protection method for digital media data that substantially obviates one or more problems due to limitations and disadvantages of the related art.

[0011] An object of the present invention is to provide a copy protection method that protects a digital media data set by allowing only compliant devices having a compliant secret key to play or read the media data set.

[0012] Another object of the present invention is to provide a copy protection method that protects a digital media data set by controlling its playing and recording processes with a digital watermarking technique.

[0013] Additional advantages, objects, and features of the invention will be set forth in part in the description which follows and in part will become apparent to those having ordinary skill in the art upon examination of the following or may be learned from practice of the invention. The objectives and other advantages of the invention may be realized and attained by the structure particularly pointed out in the written description and claims hereof as well as the appended drawings.

[0014] To achieve these objects and other advantages and in accordance with the purpose of the invention, as embodied and

broadly described herein, a first copy protection method for digital media includes encrypting an original media data set with a media key having a symmetric algorithm and encrypting the media key with each public key of compliant devices; delivering the encrypted media data set and the encrypted media key to a compliant playing device; decrypting the delivered media key with a private key of the playing device; and (d) decrypting the delivered media data set with the decrypted media key.

[0015] The first method further includes adding a player watermark to the decrypted media data set if the decrypted data set is not marked with "free copy", the player watermark containing a player identification of the playing device and player copy-control information; encrypting the watermark-added media data set with the decrypted media key and encrypting the decrypted media key with the each public key of compliant devices; and passing the encrypted media data set and media key to a compliant recording device.

[0016] In another aspect of the present invention, a second copy protection method for digital media includes encrypting an original media data set with a media key having a symmetric algorithm and encrypting the media key with each public key of compliant devices; delivering the encrypted media data set and the encrypted media key to a compliant playing device; decrypting

the delivered media key with a private key of the playing device; and decrypting the delivered media data set with the decrypted media key.

[0017] The second method further includes adding a player watermark to the decrypted media data set if the decrypted data set is not marked with "free copy", the player watermark containing a player identification of the playing device and player copy-control information; performing a compliance test through an authentication handshake process between the playing device and a displaying device; and transferring the watermark-added media data set to the displaying device only if the displaying device passes the test.

[0018] It is to be understood that both the foregoing general description and the following detailed description of the present invention are exemplary and explanatory and are intended to provide further explanation of the invention as claimed.

BRIEF DESCRIPTION OF THE DRAWINGS

[0019] The accompanying drawings, which are included to provide a further understanding of the invention and are incorporated in and constitute a part of this application, illustrate embodiment(s) of the invention and together with the

description serve to explain the principle of the invention. In the drawings;

[0020] FIG. 1 illustrates the first stage of the digital media copy control method according to the present invention; and

[0021] FIG. 2 illustrates the second and subsequent stages of the digital media copy protection method according to the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0022] Reference will now be made in detail to the preferred embodiments of the present invention, examples of which are illustrated in the accompanying drawings. Wherever possible, the same reference numbers will be used throughout the drawings to refer to the same or like parts.

[0023] A digital media copy process can be divided into two steps. First, a playing device reads (plays) a media data set, and the played data set is outputted to a displaying device or is recorded by a recording device. FIG. 1 and FIG. 2 illustrate the first stage and the second and subsequent stages of the digital media copy protection method according to the present invention, respectively. In both figures, the full lines, hatched elements, and dotted lines represent the media data streams, the result of

the protection system application, and the data streams filtered by the protection system.

[0024] When a media data set is encrypted by using a hybrid cryptographic technique, only compliant playing devices are able to play the encrypted media data set. In a hybrid cryptographic system, a media data set is encrypted with a media key (symmetric key) corresponding to a symmetric algorithm. The symmetric key is also encrypted with a public key algorithm by using the public key of a compliant playing device. Then the encrypted symmetric key and the encrypted media data set are delivered to one or more target playing devices. The encryption process of the symmetric key is performed for the public key of each compliant playing device. Each compliant playing device uses its own private key to decrypt the encrypted media key (symmetric key). The cryptographic levels of the public-key encryption of the media key and the media-key encryption of the media data set are chosen so that the encrypted data are safe enough to resist against any known types of attacks. The cryptographic system described above is called Digital Media Protection System (DMPS), which are shown in FIG. 1 and FIG. 2.

[0025] When a compliant playing device plays an original media data set, the compliant playing device is able to embed a player watermark in the played media signal if it has a

watermarking capability. The original media signal should contain an owner watermark (W1) that includes owner identification and copy control information. The player watermark includes player identification and modified copy control information derived from the owner copy control information. For any media data set marked with "free copy", the compliant playing device should not embed the player watermark.

[0026] After the compliant playing device decrypts the encrypted media data set and subsequently adds the player watermark into the media data set, the playing device passes the digital media signal to an output device, which is generally one of a digital display device and a digital recording device. When the media signal is outputted to a digital display device, the media signal should not be DMPS protected. On the other hand, when the media signal is outputted to a recording device, the media signal should be DMPS protected. That is, the media signal must include the DMPS infrastructure in order to provide compliance of the recording device with the playing device. In addition, when the media data set is transferred to the displaying device, the data set must contain a player watermark with copy control information set to "for display only".

[0027] In order to prevent any data interception between the playing and displaying devices, a copy protected digital

transmission protocol (e.g., 1394 with AKE) must be used. The protocol provides the compliance testing between the devices through an authenticated handshaking process. If the authentication of a displaying device is not approved, the media data set should not be transferred to the displaying device. Virtually, there is a chance that a generic recording device having a valid device certificate may substitute the displaying device and may mislead the AKE process. Therefore, the protection system according to the present invention may be considered as theoretically surmountable, and illegal copies may be made in such a way. Of course, the copies will contain the owner and player watermarks.

[0028] When the playing device passes the media data set to a recording device, the playing device will output the data set in the DMPS-protected form as the data set stored in the original media data set. Thus, no additional data transfer protection is required. A compliance test of the recording device is optional because any recording device will be a "dump-only" device for the data set received from the playing device.

[0029] When a legal media copy is played on a compliant playing device, Digital Media Copy Control System (DMCCS) will operate. If the media data set contains owner and player watermarks whose copy control information are not correlated with

each other, or if the player watermark is marked with "for display only", the media data set will be rejected by the playing device. When an original media data set or its copy is about to be transferred to a recording device, the playing device's DMCCS initially checks the watermark copy control information and prevents the media data set from being copied if the media data set is marked with "no copy."

[0030] A legal media data set and its copy will not be compatible with a non-compliant playing device because they are DMPS-protected. An illegal copy is incompatible with a compliant playing device for the same reason. Therefore, this feature of the present invention will stop an ordinary user from using any illegal copy of a media data set. Moreover, a player watermark contains the individual identification of every playing device so that an origin of any illegal copy can be found.

[0031] It will be apparent to those skilled in the art that various modifications and variations can be made in the present invention without departing from the spirit or scope of the inventions. Thus, it is intended that the present invention covers the modifications and variations of this invention provided they come within the scope of the appended claims and their equivalents.